REMARKS

Claim Rejections – 35 USC § 103

In Section 5 of the Office Action, the Examiner rejected claims 19-20 under 35 U.S.C. 103(a) as being unpatentable over Kaufman (US 6,178,508) in view of Krahn et al (US 2001/0027442). This rejection is traversed in that the proposed combination of references fails to teach an authorization methodology in which a user ID is compared to a list of authorized users, while both the ID and list are in any encrypted and compressed format as claimed.

The claimed invention provides an advantageous way to authenticate a user of a hand-held data process device. A list of values corresponding to authorized users is transferred to the device. The list is in the form of CRC values.

In other words, the list is both encrypted and compressed in the CRC value format.

A user ID is inputted into the device and a corresponding CRC value for the ID is calculated.

In other words, an encrypted and compressed version of the user ID is calculated in the CRC format.

Then, while both the list and the user ID are still encrypted and compressed in the CRC value format, the method compares the encrypted and compressed ID value to values in the encrypted and compressed list to determine if the ID value is authorized.

In other words, the user authentication occurs when both the list and user ID are in an encrypted and compressed format of CRC values.

The authentication methodology of the present invention provides significant advantages in the context of hand-held devices as compared to the use of full character strings. The amount of memory required to store and carry out authentication is dramatically reduced. For instance, as noted in the specification, storing 4000 strings having 18 characters would use 72,000 bytes of RAM, but compression of these into the CRC format even using 32-bit conversion only requires 16,000 bytes. And even though the data is compressed, the confidence level for the values remains quite high, e.g., only one chance in 4,294,967,296 of being incorrect in those embodiments in which 32-bit CRC values are used. Additionally, the data transfer to the device occurs faster.

In this regard, the Examiner's attention is directed to Paragraphs [66] through [72] primarily which summarize such advantages, but paragraphs [73] et seq. also describe the advantages and features of the claimed method.

The primary reference Kaufman fails to teach a method that compares an encrypted and compressed ID value to values in an encrypted and compressed list to determine if the ID value is authorized. Kaufman discloses encryption/decryption of passwords for a conventional personal computer system. In Kaufman, the user list and the inputted user ID are cryptographically hashed, BUT ARE NOT COMPRESSED. Kaufman password values are never compared to list values while both kinds of values are both encrypted and compressed.

Note, too, how Kaufman relates mainly to computer networks used by many users and not to hand-held devices. There is not much motivation for the skilled worker to migrate Kaufman to a compressed approach as claimed, inasmuch as the memory and data transfer issues associated with hand-held devices is not very germane to large network systems.

Krahn fails to cure these deficiencies. Krahn et al. discloses a method of exporting a configuration data file having a data password to a persistent configuration text file. The Examiner asserts that Krahn et al. teaches calculating a cyclic redundancy check (CRC) value and comparing the CRC value for the user identification string to the list of CRC values on the hand-held data processing device. To this assertion Applicants respectfully disagree with the Examiner.

Krahn describes a system in which data is encrypted as it is transferred among data files. It is true that user information is encrypted. However, the process of user authentication is never carried out when both the user information and the list of authorized users are in an encrypted and compressed format of CRC values. Quite simply, a comparison of an encrypted and compressed user ID is never compared to an encrypted and compressed list of authorized users for authentication purposes.

Suffering from the same deficiency as Kaufman, it is clear that Krahn is not able to cure the deficiency of Kaufman.

Further, because the Applicant's Application of CRC methods to the problem of verifying user access to a hand-held device in an efficient manner was not a logical extension to the methods of encrypting and decrypting passwords and transferring password files disclosed in Kaufman and Krahn, et al., there is no motivation or

suggestion to combine these to references to arrive at the invention of claim 19. Therefore, for at least this reason alone, claim 19 and dependent claim 20 are allowable.

In short, neither Kaufman nor Krahn et al., discloses, teaches, or suggests, alone, or in any proper combination the use of CRC calculations and values for comparison during an authentication process. Also, neither Kaufman nor Krahn et al., discloses, or teaches the transfer of a list of CRC values to a hand-held device. Thus, not all of the claim elements of claim 19 are taught or disclosed by any proper combination of the references. Applicants respectfully submit that claim 19 and its dependent claim 20 are allowable.

CONCLUSION

It is respectfully submitted that the present claims are now in condition for allowance, and early notice to that effect is earnestly solicited. In the event that a phone conference between the Examiner and the Applicants' undersigned attorney would help resolve any remaining issues in the application, the Examiner is invited to contact the attorney at (651) 275-9833.

Respectfully Submitted,

Dated: Dec. 23 , 2005   By: David B. Kagan

David B. Kagan, Reg. No. 33,406
Customer No. 33072
Phone: 651-275-9804
Fax: 651-351-2954

20830